CONTRAST
SECURITY

WEAVING SECURITY INTO THE DEVELOPERS MINDSET AND PROCESSES

REDUCING APPLICATION VULNERABILITIES AND OVERALL BUSINESS RISK

"Contrast Security has increased our level of confidence in ensuring the quality and security of our software applications. It has empowered our developers and is an integral part of our SDLC. As a result, it has enhanced developer productivity and security."

DAVID | HEAD OF APPLICATION SECURITY

AT A GLANCE

Industry: Banking & Financial Services

Location(s): United States, United Kingdom and Asia

Challenge: Quickly, continuously, and cost effectively help developers and security teams identify and remediate application vulnerabilities within their applications early in the Software Development Life Cycle (SDLC)

Solution: Contrast Assess to augment application security testing quickly and effectively, enabling the bank to "shift security to the left"

Results:
- Reduced time to pen test by 50% and optimized resources
- Empowered developers with tools to create secure code
- Increased developers' productivity
- Educated developers to better understand and reduce application code vulnerabilities
- Delivered accurate, continuous vulnerability detection and attack protection
- Accelerated software time-to-market
- Improved development operational processes
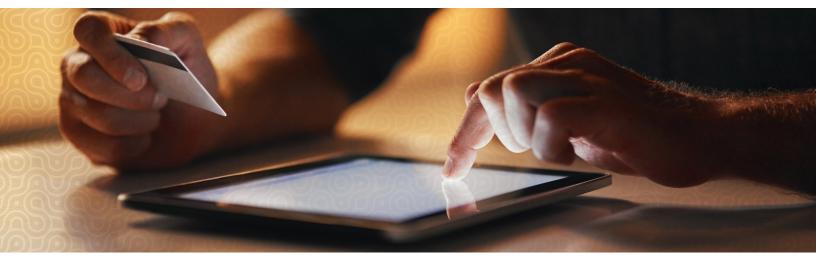- Reduced overall AppSec testing costs

OVERVIEW

Security was becoming increasingly important for one of the 10 largest banks in the world as it embarked on a process of Digital Transformation to streamline its domestic and international business.

The bank provides a fully integrated suite of financial products and services including retail, business and institutional banking, funds management, insurance, investment and brokerage services, and has more than 1,000 branches worldwide, 5,000 ATMs, over 50,000 employees, and millions of customers.

The head of the Application Security (AppSec) organization at the bank was responsible for establishing and executing the bank's AppSec capabilities and integrating security in software development. Over the last few years the AppSec team has depended on static tools to ensure the security of the software they develop in-house.

Changes in technology and the evolving threat landscape had motivated the bank to boost its defenses - requiring a cost effective, automated AppSec testing solution that addresses all their major issues.

CHALLENGES

DIGITAL TRANSFORMATION

The changing technology challenges that the bank faced could be attributed to "Digital Transformation" - with software at the heart of this major shift. The bank had utilized the latest software methodologies to transform the way they ran their businesses – better customer experiences, business efficiencies, time and cost optimization. Most importantly, the bank wanted to stay relevant and competitive in the changing digital environment.

As part of its brand and reputation, the bank delivers seamless customer experiences, in smart and innovative ways and has a reputation for excellent customer experiences, service and leadership. As part of its growth strategy, the company recognized that it needed to effectively navigate the rapid business and digital transformations that were taking place.

CONTRAST
SECURITY

INTEGRATING AGILE WITH DEVOPS

The organization's software had been developed and released at an increasingly rapid pace since the development team had combined Agile sprints with DevOps methodologies. As a result, the bank innovated faster, realized greater efficiencies and differentiated its products and services.

But, continually rolling out software at a faster rate introduces potential vulnerabilities and greater business risk. It became key for the bank to manage and balance between speed and risk.

The head of the AppSec team found that some of the bank's current AppSec tools and processes were inadequate in addressing the issues that he faced.

That gap was placing a strain on the workload of his developers:

- Code release delays caused by traditional Static (SAST) and Dynamic (DAST) Application Scanning Tools
- Scalability concerns using scanning tools for every single release
- Manual testing delays in development
- Time consuming in developer training and education

It was clear to the bank that they needed to move toward more Agile security processes.

"We compared offerings from several leading AppSec testing suppliers. Contrast Security proved to be the most attractive, being the right tool for the right job," says David, Head of Application Security.

The ease of using Contrast Assess allowed the team to seamlessly integrate into their Agile and DevOps SDLC processes, while enhancing their current security posture. Contrast Assess provided highly accurate results for developers without the dependence on experts for triage.

David adds, "Contrast Assess has been instrumental in helping us weave security into the developers' mindset as they create code."

DEVELOPING SECURE CODE

The bank currently has over 4,000 developers - comprised of internal staff, third parties and outsourced consultants including Penetration Testers (pen testers). These groups focus on the continuous development, release, maintenance and security of thousands of applications. The applications are a combination of internally developed software and off the shelf Open Source Software (OSS).

The bank had been rapidly moving toward using microservices for the platforms used by the banks numerous business units. The platforms are used across multiple business units and composed of numerous microservices - these include the bank's flagship customer retail banking internet platform, as well as their business banking and digital asset platforms.

"Users really like and rely on the Contrast product heavily. Since developers have been using Contrast and learning more about application security vulnerabilities, we have seen a significant reduction in the number of identified vulnerabilities," says David, Head of Application Security, adding that "Contrast gives us a much greater assurance about the quality and security of our code."

CONTRAST
SECURITY

INTEGRATING SECURITY WITH AGILE

The organization realized that software releases can be negatively impacted if code vulnerabilities are identified toward the end of the SDLC. This adds to increased delays and significant cost to remediate. At the bank, security practices need to keep pace with software development in Agile and DevOps environments. This shifts security from being a bottleneck to an enabler.

Contrast has provided the bank with security that fits with continuous integration and delivery (CI/CD), microservices and other development process.

"We wanted to automate and streamline our application security testing without having it slow us down in our continuous development environment," noted David.

ADDITIONAL USE CASE

Penetration Testing

The bank has relied heavily on pen testing to defend business and information systems from malicious attacks. Pen testing is a critical code assurance activity before deploying into production.

Contrast Assess was also used to supplement the bank's pen testing, chiefly focused on their major platforms. Results from Contrast's centralized management dashboard (TeamServer) were shared with internal "Red Teams" and pen testers, highlighting key vulnerabilities and providing them with swift remediation.

Contrast demonstrated that it can reduce the time for pen testing by about 50% and optimize resources required to conduct Pen tests.

"For incremental releases of code, Contrast can minimize the number of pen tests required of the code," adds the Head of Application Security, David.

RESULTS

Customer Business Benefits:

- Code created is highly secure before it is released into production environments
- Reduction in pen testing costs through optimized processes.
- AppSec team is able to deliver software security at a broader scale, and for a much lower cost, than when using legacy SAST and DAST tools.

- Application security fits seamlessly into Agile and DevOps processes and can optimize development and operational processes.
- Enabled and educated the development team by merging security with quality coding
- Increased code quality and overall performance of their developers

By intersecting development, security and operations, the bank successfully implemented a continuous and efficient way to roll out secure code. Furthermore, software can now be created and deployed much faster, without compromising security – at the speed of Agile and DevOps.

The bank can now focus on remaining highly agile, developing quality code while mitigating software risk.